File #: Int 1153-2018, **Version:** *

Int. No. 1153

By Council Members Koo, Rivera and Holden

A Local Law to amend the administrative code of the city of New York, in relation to requiring an electronic system penetration testing protocol and security briefings and reports

Be it enacted by the Council as follows:

Section 1. The title of chapter 8 of title 23 of the administrative code of the city of New York, as added by local law number 25 for the year 2016, is amended to read as follows:

CHAPTER 8

CITY WEBSITES AND ELECTRONIC SYSTEMS

§ 2. Chapter 8 of title 23 of the administrative code of the city of New York is amended by adding a new section 23-803 to read as follows:

§ 23-803 Electronic systems security testing, briefings and reports. a. For the purposes of this section, the following terms have the following meanings:

Chief information security officer. The term "chief information security officer" means the head of New York city cyber command as established by executive order number 28 for the year 2017 or any other officer or administering agency designated by the mayor to perform the same functions.

Electronic system. The term "electronic system" means any website, network, online infrastructure or internally or externally accessible electronic system constructed or maintained by or on behalf of the city.

Personal identifying information. The term "personal identifying information" shall have the same meaning as provided for the term "personal identifying information" in section 10-501 and any other identifying information, as such term is defined in section 23-1201.

b. The chief information security officer shall adopt a protocol relating to penetration testing of electronic systems. Such protocol shall use the penetration testing standards of national institute of standards and technology special publication 800-53, including all control enhancements, or any successor standard, for all physical electronic systems, and federal risk and authorization management program penetration test guidance version 1.0.1, or any successor standards, for all cloud systems; provided that the protocol may differ from such standards in specific instances when the chief information security officer determines, after consulting with experts in the security of electronic systems, that such differences will provide a more effective test, and that such differences are documented in such protocol. Such protocol shall be made publicly available online.

c. The protocol required by subdivision b shall include a standard for the testing of employees of the city as well as both internally and externally accessible electronic systems for vulnerability to social engineering exploitation. Such standard may be adopted from federal risk and authorization management program penetration test guidance version 1.0.1 or any similar standard, provided that such standard includes provisions for recording and reporting click-through rates or similar metrics.

d. The chief information security officer shall develop social engineering exploitation awareness materials and shall distribute such materials to all agency employees. Such materials shall also be distributed to all agency employees upon hiring.

e. The standard required by subdivision c shall also establish thresholds for such metrics that, when exceeded with respect to any such systems or personnel, trigger social engineering exploitation awareness material distributions or trainings and additional testing of such systems or employees of the city.

f. The protocol required by subdivision b shall be implemented by the chief information security officer, or by a vendor retained for such purpose, to regularly test for security vulnerabilities in the websites or other public facing electronic systems maintained by or on behalf of the city.

g. The chief information security officer shall conduct an annual audit of all electronic system security

practices. Such audit shall include, but not be limited to, an assessment of website security credentials, penetration vulnerabilities, and vulnerability of operating systems and firmware of electronic systems.

h. In the event of an electronic system security breach, the chief information security officer shall:

1. Immediately inform the mayor, or the mayor's designee, with a description of the date, nature and severity of the security breach, as well as a description of any data or information that may have been compromised; and

2. Immediately arrange a briefing for the speaker of council, or the speaker's designee, for the purposes of providing the following information:

(a) a description of the severity and impact of the electronic system security breach;

(b) a description of all electronic systems affected that would normally be used by the public;

(c) an estimate of time required for the issues caused by the electronic system security breach to be fixed;

(d) whether the individuals responsible for the electronic system security breach have been identified; and

(e) any resulting electronic system threats that the public should be made aware of.

i. By February 1 of each year, the chief information security officer shall submit to the speaker of the council, and make publicly available online, an electronic report that describes:

1. the implementation of this section;

2. the number of penetration vulnerabilities identified through testing performed pursuant to this section since the prior report, both citywide and by agency;

3. the number and scope of social engineering exploitation tests conducted, both citywide and by agency;

4. the percentage of such social engineering exploitation tests for which the established metric did not meet the trigger threshold established pursuant to subdivision e, both citywide and by agency;

5. the percentage of additional social engineering exploitation tests conducted pursuant to subdivision e, both citywide and by agency, for which the established metric did not meet the trigger threshold established pursuant to subdivision e;

6. a description of any social engineering exploitation awareness material distributions or trainings conducted, both citywide and by agency;

7. a description of the date, nature and severity of any resolved electronic system security breaches in the preceding year, as well as any information or data that may have been compromised; and

8. recommendations for improvement in city practices and protocols for the security of electronic systems including, but not limited to, recommendations based on the findings of the audit conducted pursuant to subdivision g.

§ 3. This local law takes effect 120 days after it becomes law, except that the office of the mayor and the department of information technology and telecommunications may take such measures prior to such date as are necessary for implementation of this local law, including the promulgation of rules.

APB/bjr
LS #6356, 6881,7823
9/26/18, 11:25 pm